EXHIBIT B

Recognized as an
American National Standard (ANSI)

IEEE Std 802.1X-2001

IEEE Standard for
Local and metropolitan area networks—

Port-Based Network Access Control

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 14 June 2001

IEEE-SA Standards Board

Approved 25 October 2001

American National Standards Institute

Abstract: *Port-based network access control makes use of the physical access characteristics of IEEE 802® Local Area Networks (LAN) infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.*
Keywords: *authentication, authorization, controlled Port, Local Area Networks, Port Access Control, uncontrolled Port*

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2001 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 13 July 2001. Printed in the United States of America.

Print: *ISBN 0-7381-2626-7* *SH94940*
PDF: *ISBN 0-7381-2927-5* *SS94940*

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

IEEE is the sole entity that may authorize the use of certification marks, trademarks, or other designations to indicate compliance with the materials set forth herein.

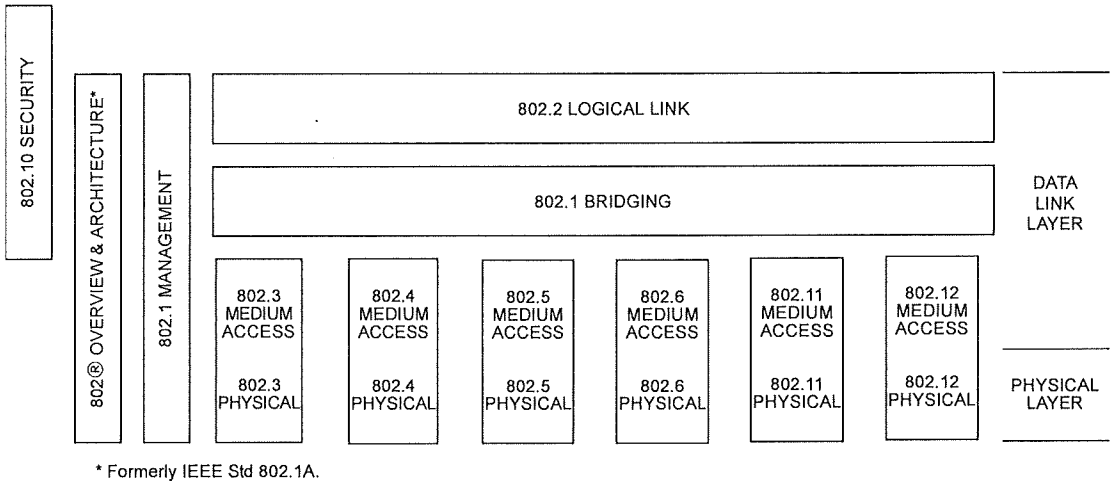
Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; (978) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

(This introduction is not part of IEEE Std 802.1X-2001, IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control.)

This standard defines a mechanism for Port-based network access control that makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

This standard is part of a family of standards for local and metropolitan area networks. The relationship between the standard and other members of the family is shown below. (The numbers in the figure refer to IEEE standard numbers.)



* Formerly IEEE Std 802.1A.

This family of standards deals with the Physical and Data Link Layers as defined by the International Organization for Standardization (ISO) Open Systems Interconnection Basic Reference Model (ISO/IEC 7498-1:1994). The access standards define several types of medium access technologies and associated physical media, each appropriate for particular applications or system objectives. Other types are under investigation.

The standards defining the technologies noted above are as follows:

• IEEE Std 802[1]:	*Overview and Architecture*. This standard provides an overview to the family of IEEE 802 Standards. This document forms part of the IEEE 802.1 scope of work.
• ANSI/IEEE Std 802.1B and 802.1K [ISO/IEC 15802-2]:	*LAN/MAN Management*. Defines an Open Systems Interconnection (OSI) management-compatible architecture, and services and protocol elements for use in a LAN/MAN environment for performing remote management.

[1]The 802 Architecture and Overview Specification, originally known as IEEE Std 802.1A, has been renumbered as IEEE Std 802. This has been done to accommodate recognition of the base standard in a family of standards. References to IEEE Std 802.1A should be considered as references to IEEE Std 802.

Copyright © 2001 IEEE. All rights reserved.

• ANSI/IEEE Std 802.1D:	*Media Access Control (MAC) Bridges*. Specifies an architecture and protocol for the [ISO/IEC 15802-3]: interconnection of IEEE 802 LANs below the MAC service boundary.
• ANSI/IEEE Std 802.1E [ISO/IEC 15802-4]:	*System Load Protocol*. Specifies a set of services and protocol for those aspects of management concerned with the loading of systems on IEEE 802 LANs.
• ANSI/IEEE Std 802.1F:	*Common Definitions and Procedures for IEEE 802 Management Information*.
• ANSI/IEEE Std 802.1G [ISO/IEC 15802-5]:	*Remote Media Access Control (MAC) Bridging*. Specifies extensions for the interconnection, using non-LAN systems communication technologies, of geographically separated IEEE 802 LANs below the level of the logical link control protocol.
• ANSI/IEEE Std 802.1H [ISO/IEC TR 11802-5]:	*Recommended Practice for Media Access Control (MAC) Bridging of Ethernet V2.0 in IEEE 802 Local Area Networks*.
• ANSI/IEEE Std 802.1Q:	*Virtual Bridged Local Area Networks*. Defines an architecture for Virtual Bridged LANs, the services provided in Virtual Bridged LANs, and the protocols and algorithms involved in the provision of those services.
• ANSI/IEEE Std 802.2 [ISO/IEC 8802-2]:	*Logical Link Control*.
• ANSI/IEEE Std 802.3 [ISO/IEC 8802-3]:	*CSMA/CD Access Method and Physical Layer Specifications*.
• ANSI/IEEE Std 802.4 [ISO/IEC 8802-4]:	*Token Bus Access Method and Physical Layer Specifications*.
• ANSI/IEEE Std 802.5 [ISO/IEC 8802-5]:	*Token Ring Access Method and Physical Layer Specifications*.
• ANSI/IEEE Std 802.6 [ISO/IEC 8802-6]:	*Distributed Queue Dual Bus Access Method and Physical Layer Specifications*.
• ANSI/IEEE Std 802.10:	*Interoperable LAN/MAN Security*. Currently approved: Secure Data Exchange (SDE).
• ANSI/IEEE Std 802.11: [ISO/IEC 8802-11]	*Wireless LAN Medium Access Control (MAC) Sublayer and Physical Layer Specifications*.
• ANSI/IEEE Std 802.12: [ISO/IEC 8802-12]	*Demand Priority Access Method, Physical Layer and Repeater Specification*.
• IEEE Std 802.15:	*Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks*.
• IEEE Std 802.16:	*Standard Air Interface for Fixed Broadband Wireless Access Systems*.
• IEEE Std 802.17:	*Resilient Packet Ring Access Method and Physical Layer Specifications*.

Copyright © 2001 IEEE. All rights reserved.

In addition to the family of standards, the following is a recommended practice for a common physical layer technology:

• IEEE Std 802.7:	*IEEE Recommended Practice for Broadband Local Area Networks.*

The reader of this standard is urged to become familiar with the complete family of standards.

Conformance test methodology

An additional standards series, identified by the number IEEE 1802, has been established to identify the conformance test methodology documents for the IEEE 802 family of standards. Thus the conformance test documents for IEEE 802.3 are numbered IEEE 1802.3, the conformance test documents for IEEE 802.5 will be 1802.5, and so on. Similarly, ISO will use ISO/IEC 18802 to number conformance test standards for ISO/IEC 8802 standards.

Participants

At the time this standard was completed, the IEEE 802.1 Working Group had the following membership:

Tony Jeffree, *Chair and Editor*
Neil Jarvis, *Vice-Chair*
Mick Seaman, *Chair, Interworking Task Group*

Les Bell
Alan Chambers
Marc Cochran
Paul Congdon
Hesham El Bakoury
Norman W. Finn
Sharam Hakimi
Bob Hott
Toyoyuki Kato
Hal Keen
Daniel Kelley
Keith Klamm
Joe Laurence
Bill Lidinsky
Yaron Nachman
LeRoy Nash
Satoshi Obara
Luc Pariseau
Anil Rijsinghani
John J. Roese
Ted Schroeder
Benjamin Schultz
Rosemary V. Slager
Andrew Smith
Michel Soerensen
Robin Tasker
Manoj Wadekar
Robert Williams

Copyright © 2001 IEEE. All rights reserved.

The following members of the balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

David J. Allred
Jacob Ben Ary
James T. Carlo
Linda T. Cheng
Keith Chow
Guru Dutt Dhingra
Thomas J. Dineen
Christos Douligeris
Sourav K. Dutta
Philip H. Enslow
Changxin Fan
John W. Fendrich
Michael A. Fischer
Richard A. Froke
Robert J. Gagliano
Gautam Garai
Alireza Ghazizahedi
Tim Godfrey
Robert M. Grow
Chris G. Guy
Simon Harrison
Osamu Ishida
Raj Jain
Kamran Jamal
Neil A. Jarvis
Anthony A. Jeffree
Stuart J. Kerry
Daniel R. Krent
Stephen Barton Kruger
Joseph Kubler
David J. Law
William Lidinsky
Randolph S. Little
Ronald Mahany
Peter Martini
Bennett Meyer
David S. Millman
James F. Mollenauer
John E. Montague
Robert Mortonson
Robert O'Hara
Donal O'Mahony
Satoshi Obara
Roger Pandanda
Vikram Punj
Gary S. Robinson
Edouard Y. Rocher
James W. Romlein
Floyd E. Ross
Jaideep Roy
Leo Sintonen
Joseph S. Skorupa
Fred J. Strauss
Jonathan R. Thatcher
Jerry A. Thrasher
Mark-Rene Uchida
Scott A. Valcourt
John Viaplana
Paul A. Willis
Forrest D. Wright
Oren Yuen

When the IEEE-SA Standards Board approved this standard on 14 June 2001, it had the following membership:

Donald N. Heirman, *Chair*
James T. Carlo, *Vice Chair*
Judith Gorman, *Secretary*

Chuck Adams
Mark D. Bowman
Clyde R. Camp
Richard DeBlasio
Harold E. Epstein
H. Landis Floyd
Jay Forster*
Howard M. Frazier
James H. Gurney
Raymond Hapeman
Richard J. Holleman
Richard H. Hulett
Lowell G. Johnson
Joseph L. Koepfinger*
Peter H. Lips
Paul J. Menchini
Daleep C. Mohla
Robert F. Munzner
Ronald C. Petersen
Malcolm V. Thaden
Geoffrey O. Thompson
Akio Tojo
Howard L. Wolfman

*Member Emeritus

Also included is the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Alan H. Cookson, *NIST Representative*
Donald R. Volzka, *TAB Representative*

Jennifer McClain Longman
IEEE Standards Project Editor

The marks "**IEEE**" and "**802**" are registered trademarks belonging to the IEEE. When using these marks to refer to The Institute of Electrical and Electronics Engineers, **802** standards or other standards, the marks should be in bold typeface and, at least once in text, use the registered trademark symbol "®".

Copyright © 2001 IEEE. All rights reserved.

Contents

Copyright © 2001 IEEE. All rights reserved.

Copyright © 2001 IEEE. All rights reserved.

it could be argued that authentication is not necessary because the Supplicant PAE has already been authenticated. However, it is possible in some environments to reinitialize a machine, bypass the normal login, and access the Authenticator System's services. To prevent an unauthorized user from accessing the Authenticator by reinitializing an authenticated machine, a Supplicant initiation of authentication is necessary upon reinitialization.

8.4.2.1 Authenticator initiation

The Authenticator PAE will typically initiate the conversation when it receives an indication that the Port has become operable. Before authentication commences, the Port state is forced to the unauthorized state.

If the Supplicant's Identity is not known, then the Authenticator PAE initiates the authentication sequence by sending an EAP-Request/Identity frame. This is typically how an Authenticator PAE will begin the authentication exchange. A Supplicant PAE receiving an EAP-Request frame from the Authenticator PAE responds with an EAP-Response frame.

Authenticator PAEs may support periodic reauthentication, and they may request that a Port reauthenticate at any time. For example, if the Authenticator System reinitializes, the authentication state can be recovered by issuing EAP-Request/Identity frames on all Ports. If a controlled Port is in the authorized state prior to reauthentication, then it will remain in that state during reauthentication. If the authentication fails for a controlled Port that was in the authorized state during reauthentication, then the controlled Port's authorization state is transitioned to unauthorized in order to control external access to that Port in accordance with the current value of the OperControlledDirections parameter (6.4).

8.4.2.2 Supplicant initiation

In order to request that the Authenticator PAE initiate authentication, the Supplicant PAE sends an EAPOL-Start packet (7.5.4). The Authenticator PAE receiving an EAPOL-Start packet responds by sending an EAP-Request/Identity packet.

8.4.3 EAPOL-Logoff

When a Supplicant wishes the Authenticator PAE to perform a logoff (i.e., to set the controlled Port state to unauthorized), the Supplicant PAE originates an EAPOL-Logoff message (7.5.4) to the Authenticator PAE. As a result, the Authenticator PAE immediately places the controlled Port in the unauthorized state.

NOTE—In general, it is advisable for the Supplicant PAE to originate an EAPOL-Logoff in any circumstances in which the user of the Supplicant System has logged off (in the case of an end station), or in which the operation of the Supplicant System has been reconfigured in a manner that would invalidate any previous authentication results (for example, a management change that affects the Supplicant System's identity, or its authorization to use the services of the Authenticator's System).

8.4.4 Timing out authorization state information

Authenticator PAEs can time out the authorization state information on a periodic basis by means of the Reauthentication Timer State Machine (8.5.7). The time period for such timeouts is reAuthPeriod seconds since the last time that the authorization state was confirmed. The state variable reAuthEnabled controls whether periodic reauthentication takes place.

Reauthentication can be enabled and disabled, and the reAuthPeriod modified, by management. The default settings are for the reAuthPeriod to be 3600 s (one hour) and for reauthentication to be disabled.

NOTE—As with Authenticator and Supplicant initiated reauthentication, the implications of setting this to a lower value should be carefully thought out before proceeding. The value chosen will be affected by the reliability with which the MAC associated with the Port can detect and indicate MAC enabled/disabled conditions. If the Port's detection of MAC state is reliable, then longer timeout values may be appropriate.

Copyright © 2001 IEEE. All rights reserved.

9.4.1.3 Reauthenticate

9.4.1.3.1 Purpose

To cause the Authenticator PAE state machine for the Port to reauthenticate the Supplicant.

9.4.1.3.2 Inputs

a) **Port number.** The identification number assigned to the Port by the System in which the Port resides.

9.4.1.3.3 Outputs

None.

9.4.1.3.4 Effect

This operation causes the reauthenticate variable (8.5.2.2) for the Port's Authenticator PAE state machine to be set TRUE.

9.4.2 Authenticator Statistics

The Authenticator Statistics managed object models the operations that modify, or enquire about, the statistics associated with the operation of the Authenticator. There is a single Authenticator Statistics managed object for each Port that supports Authenticator functionality.

The management operations that can be performed on the Authenticator Statistics managed object are as follows:

— Read Authenticator Statistics (9.4.2.1)

9.4.2.1 Read Authenticator Statistics

9.4.2.1.1 Purpose

To solicit statistical information regarding the operation of the Authenticator associated with a Port.

9.4.2.1.2 Inputs

— **Port number.** The identification number assigned to the Port by the System in which the Port resides.

9.4.2.1.3 Outputs

a) **Port number.** The identification number assigned to the Port by the System in which the Port resides.

b) **EAPOL frames received.** The number of valid EAPOL frames of any type that have been received by this Authenticator.

c) **EAPOL frames transmitted.** The number of EAPOL frames of any type that have been transmitted by this Authenticator.

d) **EAPOL Start frames received.** The number of EAPOL Start frames that have been received by this Authenticator.

Copyright © 2001 IEEE. All rights reserved.

e) **authAuthSuccessWhileAuthenticating** (see 8.5.4.2.4 for the definition of this counter).

f) **authAuthTimeoutsWhileAuthenticating** (see 8.5.4.2.5 for the definition of this counter).

g) **authAuthFailWhileAuthenticating** (see 8.5.4.2.6 for the definition of this counter).

h) **authAuthReauthsWhileAuthenticating** (see 8.5.4.2.7 for the definition of this counter).

i) **authAuthEapStartsWhileAuthenticating** (see 8.5.4.2.8 for the definition of this counter).

j) **authAuthEapLogoffWhileAuthenticating** (see 8.5.4.2.9 for the definition of this counter).

k) **authAuthReauthsWhileAuthenticated** (see 8.5.4.2.10 for the definition of this counter).

l) **authAuthEapStartsWhileAuthenticated** (see 8.5.4.2.11 for the definition of this counter).

m) **authAuthEapLogoffWhileAuthenticated** (see 8.5.4.2.12 for the definition of this counter).

n) **backendResponses** (see 8.5.8.2.1 for the definition of this counter).

o) **backendAccessChallenges** (see 8.5.8.2.2 for the definition of this counter).

p) **backendOtherRequestsToSupplicant** (see 8.5.8.2.3 for the definition of this counter).

q) **backendNonNakResponsesFromSupplicant** (see 8.5.8.2.4 for the definition of this counter).

r) **backendAuthSuccesses** (see 8.5.8.2.5 for the definition of this counter).

s) **backendAuthFails** (see 8.5.8.2.6 for the definition of this counter).

9.4.4 Authenticator Session Statistics

The Authenticator Session Statistics managed object models the operations that modify, or enquire about, the statistics associated with a Session. There is a single Authenticator Session Statistics managed object for each Port that supports Authenticator functionality.

The managed object records the statistics for the current session (if there is an active session, i.e., the portStatus variable for the Authenticator PAE state machine is set to Authorized), or the previous session (if there is no active session, i.e., the portStatus variable for the Authenticator PAE state machine is set to Unauthorized).

The management operations that can be performed on the Authenticator Session Statistics managed object are as follows:

— Read Authenticator Statistics (9.4.2.1)

The session statistics associated with each Port are maintained for the duration of a session, i.e., for the period of time during which the Port is authenticated. The statistics parameters are initialized, by setting their values to zero, at the point where the portStatus variable (see 8.5.2.2, 8.5.4) of the Authenticator PAE State machine transitions from Unauthorized to Authorized. While the value of portStatus remains Authorized, the session statistics are updated in accordance with their individual parameter definitions. The values of the session statistics are frozen, and not further updated, when the value of portStatus becomes Unauthorized.

NOTE—The session parameters identified here are suitable for communication to a RADIUS server at the end of a session for accounting purposes (see draft-ietf-radius-accounting-v2); defining them in this way makes the current session parameter values available to management before the end of a session. The parameters defined may also be suitable for communication using backend authentication mechanisms supported by protocols other than RADIUS.

Copyright © 2001 IEEE. All rights reserved.

9.5.2 Supplicant Statistics

The Supplicant Statistics managed object models the operations that modify, or enquire about, the statistics associated with the operation of the Supplicant. There is a single Supplicant Statistics managed object for each Port that supports Supplicant functionality.

The management operations that can be performed on the Supplicant Statistics managed object are as follows:

— Read Supplicant Statistics (9.5.2.1)

9.5.2.1 Read Supplicant Statistics

9.5.2.1.1 Purpose

To solicit statistical information regarding the operation of the Supplicant associated with a Port.

9.5.2.1.2 Inputs

— **Port number.** The identification number assigned to the Port by the System in which the Port resides.

9.5.2.1.3 Outputs

a) **Port number.** The identification number assigned to the Port by the System in which the Port resides.

b) **EAPOL frames received.** The number of EAPOL frames of any type that have been received by this Supplicant.

c) **EAPOL frames transmitted.** The number of EAPOL frames of any type that have been transmitted by this Supplicant.

d) **EAPOL Start frames transmitted.** The number of EAPOL Start frames that have been transmitted by this Supplicant.

e) **EAPOL Logoff frames transmitted.** The number of EAPOL Logoff frames that have been transmitted by this Supplicant.

f) **EAP Resp/Id frames transmitted.** The number of EAP Resp/Id frames that have been transmitted by this Supplicant.

g) **EAP Response frames transmitted.** The number of valid EAP Response frames (other than Resp/Id frames) that have been transmitted by this Supplicant.

h) **EAP Req/Id frames received.** The number of EAP Req/Id frames that have been received by this Supplicant.

i) **EAP Request frames received.** The number of EAP Request frames (other than Rq/Id frames) that have been received by this Supplicant.

j) **Invalid EAPOL frames received.** The number of EAPOL frames that have been received by this Supplicant in which the frame type is not recognized.

k) **EAP length error frames received.** The number of EAPOL frames that have been received by this Supplicant in which the Packet Body Length field (7.5.5) is invalid.

l) **Last EAPOL frame version.** The protocol version number carried in the most recently received EAPOL frame.

m) **Last EAPOL frame source.** The source MAC address carried in the most recently received EAPOL frame.

Copyright © 2001 IEEE. All rights reserved.

10.4.1 Relationship to the managed objects defined in Clause 9

Table 10-1 contains cross-references between the objects defined in Clause 9 and the MIB objects defined in this clause.

Table 10-1—Managed object cross-reference table

Definition in Clause 9	MIB object(s)
9.6.1 System Configuration	**dot1xPaeSystem**
Port number	dot1xPaePortNumber (table index)
SystemAuthControl	dot1xPaeSystemAuthControl
Protocol version	dot1xPaePortProtocolVersion
PAE capabilities	dot1xPaePortCapabilities
Initialize Port	dot1xPaePortInitialize
9.4.1 Authenticator Configuration	**dot1xAuthConfigTable**
Port number	dot1xPaePortNumber (table index)
Authenticator PAE State	dot1xAuthPaeState
Backend Authentication State	dot1xAuthBackendAuthState
AdminControlledDirections	dot1xAuthAdminControlledDirections
OperControlledDirections	dot1xAuthOperControlledDirections
AuthControlledPortStatus	dot1xAuthAuthControlledPortStatus
AuthControlledPortControl	dot1xAuthAuthControlledPortControl
quietPeriod	dot1xAuthQuietPeriod
txPeriod	dot1xAuthTxPeriod
suppTimeout	dot1xAuthSuppTimeout
serverTimeout	dot1xAuthServerTimeout
maxReq	dot1xAuthMaxReq
reAuthPeriod	dot1xAuthReAuthPeriod
reAuthEnabled	dot1xAuthReAuthEnabled
KeyTransmissionEnabled	dot1xAuthKeyTxEnabled
Reauthenticate	dot1xPaePortReauthenticate
9.4.2 Authenticator Statistics	**dot1xAuthStatsTable**
Port number	dot1xPaePortNumber (table index)
EAPOL frames received	dot1xAuthEapolFramesRx
EAPOL frames transmitted	dot1xAuthEapolFramesTx
EAPOL Start frames received	dot1xAuthEapolStartFramesRx

Copyright © 2001 IEEE. All rights reserved.

Table 10-1—Managed object cross-reference table *(continued)*

Definition in Clause 9	MIB object(s)
EAPOL Logoff frames received	dot1xAuthEapolLogoffFramesRx
EAP Resp/Id frames received	dot1xAuthEapolRespIdFramesRx
EAP Response frames received	dot1xAuthEapolRespFramesRx
EAP Req/Id frames transmitted	dot1xAuthEapolReqIdFramesTx
EAP Request frames transmitted	dot1xAuthEapolReqFramesTx
Invalid EAPOL frames received	dot1xAuthInvalidEapolFramesRx
EAP length error frames received	dot1xAuthEapLengthErrorFramesRx
Last EAPOL frame version	dot1xAuthLastEapolFrameVersion
Last EAPOL frame source	dot1xAuthLastEapolFrameSource
9.4.3 Authenticator Diagnostics	**dot1xAuthDiagTable**
authEntersConnecting	dot1xAuthEntersConnecting
authEapLogoffsWhileConnecting	dot1xAuthEapLogoffsWhileConnecting
authEntersAutheniticating	dot1xAuthEntersAuthenticating
authAuthSuccessWhileAuthenticating	dot1xAuthAuthSuccessWhileAuthenticating
authAuthTimeoutsWhileAuthenticating	dot1xAuthAuthTimeoutsWhileAuthenticating
authAuthFailWhileAuthenticating	dot1xAuthAuthFailWhileAuthenticating
authAuthReauthsWhileAuthenticating	dot1xAuthAuthReauthsWhileAuthenticating
authAuthEapStartsWhileAuthenticating	dot1xAuthAuthEapStartsWhileAuthenticating
authAuthLogoffWhileAuthenticating	dot1xAuthAuthEapLogoffWhileAuthenticating
authAuthReauthsWhileAuthenticated	dot1xAuthAuthReauthsWhileAuthenticated
authAuthEapStartsWhileAuthenticated	dot1xAuthAuthEapStartsWhileAuthenticated
authAuthLogoffWhileAuthenticated	dot1xAuthAuthEapLogoffWhileAuthenticated
backendResponses	dot1xAuthBackendResponses
backendAccessChallenges	dot1xAuthBackendAccessChallenges
backendOtherRequestsToSupplicant	dot1xAuthBackendOtherRequestsToSupplicant
backendNonNakResponsesFromSupplicant	dot1xAuthBackendNonNakResponsesFromSupplicant
backendAuthSuccesses	dot1xAuthBackendAuthSuccesses
backendAuthFails	dot1xAuthBackendAuthFails
9.4.4 Authenticator Session Statistics	**dot1xAuthSessionStatsTable**
Port number	dot1xPaePortNumber (table index)
Session Octets Received	dot1xAuthSessionOctetsRx

Copyright © 2001 IEEE. All rights reserved.

Table 10-1—Managed object cross-reference table *(continued)*

Definition in Clause 9	MIB object(s)
Session Octets Transmitted	dot1xAuthSessionOctetsTx
Session Frames Received	dot1xAuthSessionFramesRx
Session Frames Transmitted	dot1xAuthSessionFramesTx
Session Identifier	dot1xAuthSessionId
Session Authentication Method	dot1xAuthSessionAuthenticMethod
Session Time	dot1xAuthSessionTime
Session Terminate Cause	dot1xAuthSessionTerminateCause
Session User Name	dot1xAuthSessionUserName
9.5.1 Supplicant Configuration	**dot1xSuppConfigTable**
Port number	dot1xPaePortNumber (table index)
Supplicant PAE State	dot1xSuppPaeState
heldPeriod	dot1xSuppHeldPeriod
authPeriod	dot1xSuppAuthPeriod
startPeriod	dot1xSuppStartPeriod
maxStart	dot1xSuppMaxStart
9.5.2 Supplicant Statistics	**dot1xSuppStatsTable**
Port number	dot1xPaePortNumber (table index)
EAPOL frames received	dot1xSuppEapolFramesRx
EAPOL frames transmitted	dot1xSuppEapolFramesTx
EAPOL Start frames transmitted	dot1xSuppEapolStartFramesTx
EAPOL Logoff frames transmitted	dot1xSuppEapolLogoffFramesTx
EAP Resp/Id frames transmitted	dot1xSuppEapolRespIdFramesTx
EAP Response frames transmitted	dot1xSuppEapolRespFramesTx
EAP Req/Id frames received	dot1xSuppEapolReqIdFramesRx
EAP Request frames received	dot1xSuppEapolReqFramesRx
Invalid EAPOL frames received	dot1xSuppInvalidEapolFramesRx
EAP length error frames received	dot1xSuppEapLengthErrorFramesRx
Last EAPOL frame version	dot1xSuppLastEapolFrameVersion
Last EAPOL frame source	dot1xSuppLastEapolFrameSource

Copyright © 2001 IEEE. All rights reserved.